OFFICIAL

Joint Committee Public Accounts and Audit – Wednesday 15 September 2021

Answers to Questions on Notice

Department/Agency: Australian Signals Directorate
Inquiry: Inquiry into the *Auditor-General's reports Nos 25 and 40 (2020-21)*
Date of inquiry: 15 September 2021
Committee Member: Ms Lucy Wicks, Chair
Type of question: Hansard
Date set by the committee for the return of answer: 15 October 2021

Question 1

1. ***In July of this year, Congress directed the US Department of Defense (DoD) to comprehensively***

   "assess the risks and threats posed by quantum technologies to national security systems as well as strategies, plans and investments needed to mitigate risks toward these systems".

   Further, the National Defence Authorisation Act for FY21 directs to DoD on preparations for quantum computing, including:

   A. ***an identification and prioritization of critical national security systems at risk;***

   B. ***an assessment of NIST standards for quantum-resistant cryptography and their application to cryptographic requirements of the Department of Defense;***

   C. ***an assessment of the feasibility of alternate quantum-resistant algorithms and features;***

   D. ***a description of any funding shortfalls in public and private developmental efforts relating to quantum-resistant cryptography, standards, and models; and***

   E. ***develop recommendations for research, development, and acquisition activities, including resourcing schedules, for securing the critical national security systems against quantum computing code-breaking capabilities.***

Has ASD been asked by government to assess the Commonwealth's quantum vulnerabilities? Are you aware whether any entity in the government has?

Response:

In accordance with ASD's function as the national cyber security and cryptographic authority, ASD continually assess the Commonwealth's cybersecurity threats and vulnerabilities – including those posed by quantum computing. ASD is evaluating the security of candidate post-quantum cryptography and monitoring the progress of public standardisation efforts such as the Post-

Quantum Cryptography Standardisation Process that is being undertaken by the United States National Institute of Standards and Technology (NIST).

ASD works with international partners and across government, including the Critical Technologies Policy Coordination Office (CTPCO) in the Department of the Prime Minister and Cabinet to monitor and advise on the development and security of critical technologies, including quantum.

Question 2

In its report The Quantum Threat to Cybersecurity: Looking through the prism of post-quantum cryptography the CSIRO notes that based on the range of expert estimates for when cryptographically relevant quantum computing will be developed

"a reasonable recommendation would be to migrate to post-quantum cryptography within the next 10 years. Given the standardisation and development cycle for security products, it means we need to be acting with urgency now."

Does ASD agree with this assessment?

Response:

ASD is evaluating the security of candidate post quantum cryptography and monitoring the progress of public standardisation efforts, such as the National Institute of Standards and Technology (NIST)'s Post-Quantum Cryptography Standardisation Process. The completion of NIST's standardisation process will be a key milestone on the transition to secure post quantum cryptography.

Question 3

ASD's view, what are commonwealth entities likely going to need to do to prepare for a post quantum world?

Response:

ASD advice and guidance is regularly updated to ensure the advice is contemporary, contestable and actionable. The Information Security Manual (ISM) is regularly updated and contains guidelines for using cryptography. Commonwealth entities should continue to apply ASD cyber security guidance as appropriate to their risk profile and in accordance with the Protective Security Policy Framework (PSPF).

Question 4

Does ASD have a view on the length of time it would take to implement controls to protect Commonwealth entities IT systems and data holdings against quantum computing enabled attacks? Has this view been provided to government?

Response:

The length of time required to implement post-quantum cryptography will vary greatly depending on a Commonwealth entity's cyber security maturity and the availability of suitable commercial implementations of post-quantum encryption schemes. The finalisation of National Institute of Standards and Technology (NIST)'s Post-Quantum Cryptography Standardisation Process is a key first step.

Commonwealth entities should continue to apply ASD cyber security guidance as appropriate to their risk profile and in accordance with the Protective Security Policy Framework (PSPF). ASD advice and guidance is regularly updated to ensure the advice is contemporary, contestable and actionable.

Question 5

Following changes to the ISM in March 2019, organisations transmitting and/or storing SECRET or TOP SECRET information were no longer advised to consult with ACSC for advice on post-quantum security.

What precipitated the removal of the recommendation that organisations consult with the ACSC for advice?

Response:

ASD updated the Information Security manual in April 2019 to align the ISM with the United States Committee on National Security Systems (CNSS) advice anticipating the need to shift to quantum-resistant cryptography, maintain interoperability, and provide a clear transition path to post-quantum algorithms when they are standardised by the United States' National Institute of Standards and Technology (NIST).

This update provided greater clarity on the protection of highly classified information, which negated the recommendation to consult with the ACSC on post-quantum considerations.

Question 6

Prior to removal of this advice, how many entities contacted the ACSC for advice on post-quantum security?

Response:

As the national cyber and cryptographic authority, ASD is regularly contacted by a variety of government and non-government entities for advice, including on post-quantum security.

Question 7

What are ASD's views on Commonwealth entity awareness of the risks posed by quantum computing to current cryptographic systems used by commonwealth entities? Has any systematic audit been undertaken or awareness/preparedness? Is there a strategy here for transitioning commonwealth cyber security to a post quantum world?

Response:

Commonwealth entities should continue to apply ASD cyber security guidance as appropriate to their risk profile and in accordance with the Protective Security Policy Framework (PSPF). ASD advice and guidance is regularly updated to ensure the advice is contemporary, contestable and actionable, including through the regular Chief Information Officer / Chief Information Security Officer (CIO/CISO) Forum.

Question 8

In May 2019 the ISM was updated to give preference to using Commercial National Security Algorithm Suite algorithms wherever possible:

> *Security Control: 1468; Revision: 4; Updated: May-19; Applicability: S, TS; Priority: Should*
> *Preference is given to using the CNSA Suite algorithms and key sizes where possible.*

Why was the use of CNSA Suite algorithms an optional control and not a mandatory control?

Response:

ASD updated the Information Security Manual (ISM) in May 2019, to include the Commercial National Security Agency (CNSA) suite of approved algorithms and key sizes. Under the ISM's risk-based framework, these algorithms were recommended as an optional control to support interoperability while maintaining equivalent security for protecting sensitive information.

Question 9

Is ASD's view that CNSA Suite algorithms address the threat posed by quantum computing?

a. ***Is the use of these algorithms a permanent solution, or do you agree with the NSA's assessment that it's a transitional solution?***
b. ***For how long does ASD expect to recommend the CNSA Suite transitional algorithms?***

Response:

CNSA suite algorithms will remain practically secure further into the future than other alternatives. The completion of National Institute of Standards and Technology (NIST)'s standardisation process will be a key milestone towards to secure post quantum cryptography. Algorithms identified by NIST's process are likely to replace the current CNSA suite.

ASD Approved Cryptographic Algorithms (AACA), which includes the CNSA suite, are updated to keep pace with changing technology and emerging threats. This includes appropriate alignment with post-quantum standards when they become available.

Question 10

Does ASD have a view on how many years will it be before a quantum computer of sufficient power to break non-CNSA Suite encryption protocols is built? Has this view been shared with government?

Response:

Estimates vary significantly as to when a cryptographically relevant quantum computer might be developed. ASD is working across government and with international partners to monitor the progress of quantum computing technology.

Question 11

What work has ASD done to ensure that secret or top-secret systems that have not implemented CNSA Suite algorithms are resilient to quantum computing?

Response:

System owners for SECRET and TOP SECRET systems implement a range of security controls to manage their risks and protect sensitive information, including cryptography. Systems undergo rigorous certification and accreditation processes which include evaluation of cryptographic systems.

Question 12

What work has ASD done to ensure that sensitive information which falls below this threshold of requiring CNSA Suite algorithms are resilient to quantum computing?

Response:

Commonwealth entities are responsible for managing their own cyber security risk and implementing appropriate ASD cyber security guidance as appropriate to their risk profiles, systems, interoperability requirements and in accordance with the PSPF. This includes consideration of whether the use of CNSA algorithms is appropriate to protect their information holdings.

Question 13

In a major report on US government cyber security released in March of this year, the US Government Accountability Office (GAO) called on the Department of Homeland Security and Office of Management and Budget to identify and prioritize initiatives to understand the Federal government's vulnerabilities to quantum computing outside the defence and security agencies and to migrate to quantum-resistant encryption.

Is ASD aware of any similar initiative within the Commonwealth Government?

Response:

ASD works with international partners and across government, including the Critical Technologies Policy Coordination Office (CTPCO) in the Department of the Prime Minister and Cabinet to monitor and advise on the development and security of critical technologies, including quantum.

ASD provides cyber security advice and guidance to Commonwealth entities, however entities are responsible under the Protective Security Policy Framework (PSPF) for implementing their own security controls.

Question 14

The Belfer Center's report* Quantum Computing and Cyber Security *has recommended that governments incentive wide-scale adoption of new encryption standards (recommendation 5).

The US Department of Defense has also been directed to undertake

"an assessment of NIST standards for quantum-resistant cryptography and their application to cryptographic requirements of the Department of Defense"

Has ASD provided advice to the government on the National Institute of Standards and Technology's Post-Quantum Cryptograph Standardisation Program and the applicability of shortlisted candidates to the cryptographic requirements of Commonwealth entities?

Response:

ASD provides technical cyber security advice to Government and industry through the Information Security Manual and other publications.

ASD advice and guidance is regularly updated to keep pace with changing technology and emerging threats. ASD is evaluating the security of candidate post quantum cryptography and monitoring the progress of public standardisation efforts. The completion of NIST's standardisation process will further inform the transition to secure post quantum cryptography.

Question 15

The Australian Strategic Policy Institute's special report The impact of quantum technologies on secure communications recommends that Australia build an international presence in quantum communications.

What work is ASD undertaking to contribute to the development of quantum communication accreditations and standards?

Response:

ASD works with international partners and across government, including the Critical Technologies Policy Coordination Office (CTPCO) in the Department of the Prime Minister and Cabinet to monitor and advise on the development and security of critical technologies, including quantum.

Question 16

Comparable jurisdictions are making significant investments in quantum technology as part of their COVID-19 recovery. For example, China ($13bn), Japan ($1.3bn), US ($2.6bn), Germany ($3.6bn), France ($2.9bn), India ($1.3bn), the Netherlands ($950m), the UK ($660m) and others.

Has ASD provided advice or recommendations to government on Australia's current spend on quantum research?

Response:

ASD's role as the national cyber and cryptologic authority is to provide cyber security advice and lead Australian Government's operational cyber security capability. ASD continues to provide technical cyber security advice to inform broader government initiatives relating to current critical technology priorities, including quantum.

Question 17

In 2019 Japan and the US signed the Tokyo Statement on Quantum Cooperation.

The Australian Strategic Policy Institute's* An Australian Strategy for the Quantum Revolution *also recommends formalising a partnership on quantum research with the US.

Has ASD provided advice to government on formalising research partnerships with the US or any other ally?

Response:

ASD continues to work with our international partners to prepare for a post-quantum world.

AUKUS is furthering collaboration between Australia's key strategic partners, the United Kingdom and the United States on enhancing our joint capabilities and interoperability across a range of technologies, including quantum.

Question 18

In The Quantum Threat to Cybersecurity: Looking through the prism of post-quantum cryptography the CSIRSO also notes that:

"if a system that requires data to remain private for a long time then one should consider urgently migrating to post-quantum encryption schemes... As an intermediate step one might also consider "hybrid" schemes, which combine both pre-quantum and post-quantum cryptography.

What are the ASD's views on the viability of hybridised encryption?

Response:

ASD does not recommend hybridised encryption methods. The CNSA Algorithm suite provides effective security as a transitional solution until a permanent post-quantum solution is available from the National Institute of Standards and Technology (NIST)'s Post-Quantum Cryptography Standardisation Process.